DURIE TANGRI LLP
DARALYN J. DURIE (SBN 169825)
ddurie@durietangri.com
RAGESH K. TANGRI (SBN 159477)
rtangri@durietangri.com
RYAN M. KENT (SBN 220441)
rkent@durietangri.com
217 Leidesdorff Street
San Francisco, CA 94111-3007
Telephone: (415) 362-6666
Facsimile: (415) 236-6300

Attorneys for Defendants - Counterclaim Plaintiff
PALO ALTO NETWORKS, INC. and Defendant
PATRICK R. BROGAN

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

FORTINET, INC.,

Plaintiff,

v.

PALO ALTO NETWORKS, INC., and PATRICK R. BROGAN,

Defendants.

AND RELATED COUNTERCLAIMS.

Case No. 09-CV-00036-RMW (PVT)

PALO ALTO NETWORKS' RESPONSIVE CLAIM CONSTRUCTION BRIEF

Date: July 14, 2010
Time: 9:00 a.m.
Ctrm: 6, 4th Floor
Judge: Honorable Ronald M. Whyte

TABLE OF CONTENTS

TABLE OF CONTENTS (CON'T)

PAGE NO.

TABLE OF AUTHORITIES

PAGE NO.

Cases

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

The parties have narrowed their claim construction disputes to eight. They boil down to questions like:

- "What does 'upon' mean?"
- "Do you 'forward' something when you don't send it anywhere?"
- "Is flow learning the process of learning about a flow, or populating an entry with the result of that learning process?"
- "Can something be 'prescribed' if it isn't the result of some determination in advance?"

In some cases, Fortinet has proposed claim constructions that significantly change the meaning of the claims, such as by replacing the word "prescribed" with the word "recognized." In other cases, Fortinet has declined to provide constructions at all, contending that the claim is understandable as written to a person of skill in the art. That is not the relevant inquiry. In each case, PAN has proffered constructions that try to clarify, but not change, the plain meaning of the claims.

II. FACTUAL BACKGROUND

A. The Fortinet Patents

1. The '974 Patent

U.S. Patent No. 6,580,974 ("'974 patent") relates to one way for a firewall[1] to determine the application (such as Skype versus Yahoo! Instant Messenger versus electronic mail) associated with a given session.[2] The firewall may not be able to determine the application merely by looking at the first packet in the session. However, it may be able to determine, for example, that the initial packet contains the content "05 02 00 02," indicating that the session uses the SOCKS5 protocol. *See* '974 Patent, Fig. 3G, attached to the Declaration of Ryan M. Kent in Support of Palo Alto Networks' Responsive Claim Construction Brief ("Kent Decl.") as Exhibit 1. It can then eliminate from consideration applications that

[1] A firewall is like a gateway between the public internet and a private network (such as a corporate network). As traffic arrives from the internet to the private network, the firewall must decide what to do with that traffic, including whether to permit the traffic to pass into the private network, to redirect the traffic to another destination or to deny the traffic entry into the private network altogether.

[2] A session is a group of related packets going back and forth between the same two computers.

cannot be used with the SOCKS5 protocol, such as certain peer-to-peer (P2P) file sharing applications, by what the patent refers to as a "negative classification for a session of not being of a particular other classification." Kent Decl., Ex. 7, 12/18/08 Amendment at 7. When the firewall receives subsequent packets in the same session, it can analyze those packets more quickly by "classifying the second packet of the session by eliminating the other classification from consideration." In the example given above, the firewall doesn't need to check whether future packets might be associated with P2P file sharing applications, having already eliminated those classifications from consideration.

During the prosecution history, the applicant argued that these elements were not found in the prior art references before the examiner. The examiner allowed the claims only after requiring that these "eliminating" and "classifying" limitations be incorporated from the dependent claims into the independent claims, where they provided the basis for the reasons for allowance. *See* Kent Decl., Ex. 7, 12/18/2008 Amendment at 7; Ex. 8, Notice of Allowability at 2-3.

2. The '125 and '311 Patents

U.S. Patent Nos. 7,376,125 ("'125 patent") and 7,177,311 ("'311patent") disclose one way to use prior classification results in classifying new, related packets in the same flow.[3] The claims of both patents require a "flow cache" that stores entries identifying prior flows and how packets belonging to those flows should be treated. Kent Decl., Ex. 2, '125 patent at 15:60-18:3; Kent Decl., Ex. 3, '311 patent at 15:1-65. When the system receives a new packet, it first looks to see whether the flow associated with that packet matches a flow that is stored in the flow cache. *Id*. When there is a corresponding entry in the flow cache, there is "a flow cache hit," and the retrieved flow cache entry dictates how the packet should be handled. *Id*. On the other hand, when there is "a packet flow cache miss," the system identifies that there is a new flow and "upon successful allocation of a new entry of the packet flow cache for the new VR flow" the "packet is forward[ed] . . . to software on the processor for flow learning." *Id.*

[3] A flow is a series of packets from one source to one destination—one half of a session. Because packets within a given flow have the same source and destination, a network device typically can treat packets within a given flow the same way.

3. The '990 Patent

U.S. Patent No. 7,519,990 ("'990 patent") discloses one way to engage in the "flow learning" required by the '125 and '311 patents. When there is a flow cache miss, the device needs to process the traffic further to figure out where that traffic should go. This was known in the prior art. The '990 patent claims an alleged improvement over the prior art: dividing the firewall's processing functions between *two* processors based on the network traffic's protocol. *See* Kent Decl., Ex. 9, 2/25/09 Notice of Allowance at 2-3. The first processor is configured to "receive network traffic content" and determine when that content matches a prescribed protocol associated with content desired to be detected (such as malware and the like). Kent Decl., Ex. 4, '990 patent at 23:27-32. Based on that determination, the first processor will either "store the network traffic content in a stack when the protocol of the network traffic content matches the prescribed protocol" (if the content needs further inspection) or "perform filtering of the network traffic if the type of the network traffic content does not match the prescribed type" (if it does not need further analysis). *Id.* at 23:33-38. The second processor is "associated with the stack" and will look at the content of the traffic stored in the stack to determine how the content should be handled. *Id.* at 23:38-43. In other words, if the traffic doesn't match the prescribed protocol, the first processor will handle the traffic itself. But if the traffic does match a prescribed protocol, the computationally intensive tasks associated with learning about the flow to figure out whether it has undesirable content can be off-loaded to a second processor.

B. PAN's Patent[4]

The '272 patent is drawn to a method and device for routing communications, including telephone calls as well as "facsimile messages or other printed documents, electronic mail messages, instant electronic messages, or any other human readable or computer readable communication." Kent Decl., Ex. 5, '272 patent at 12:35-38. The invention focuses on routing communications that have

[4] Fortinet claims that PAN is nothing more than a Fortinet copycat. Nothing could be further from the truth. PAN was founded in 2005 by Nir Zuk, who has been a key innovator in firewall technology for more than 15 years. Starting in 1994, six years before Fortinet was even founded, Zuk was Principal Engineer at Check Point Software Technologies, where he invented the stateful firewall technology on which both Fortinet's and PAN's products build. Declaration of Nir Zuk in Support of Motion for Summary Judgment of Non-Infringement of the '990 Patent at ¶ 2.

"content for an unknown destination."

III. ARGUMENT

A. AGREED CLAIM CONSTRUCTIONS

The parties have agreed upon the following constructions, which include one additional term ("stack") that was added since the filing of the Joint Claim Construction Prehearing Statement.

TERM OR PHRASE	AGREED CONSTRUCTION
predetermined value set ('272 patent)	one or more values determined in advance
processor ('990 patent)	circuitry for processing
a stack ('990 patent)	memory for temporary storage

B. CONSTRUCTION OF THE DISPUTED CLAIM TERMS

1. "Upon successful allocation of a new entry of the packet flow cache for the new VR flow, forwarding the packet to software on the processor for flow learning" ('125 claims 1, 3 and '311 claims 1, 9, 17)

TERM OR PHRASE	FORTINET'S PROPOSED CONSTRUCTION AND SUPPORT	PAN'S PROPOSED CONSTRUCTION AND SUPPORT
upon successful allocation of a new entry of the packet flow cache for the new VR flow, forwarding the packet to software on the processor for flow learning ('125 and '311 patents)	upon successful allocation of a new entry of the packet flow cache for the new VR flow, forwarding the packet to software on the processor for populating the new entry "packet flow cache" is "memory for temporarily storing information about packet flows"	after the successful creation of a new entry identifying the new VR flow in the packet flow cache, the packet is forwarded to software on a separate processor in order to determine how packets in this flow should be treated "packet flow cache" is "an intermediate memory location temporarily storing information about a subset of packet flows for rapid access"

Fortinet's proposed construction of this phrase replaces the term "flow learning" with "populating the new entry." There are two problems with this approach. First, the rest of the phrase is not self-explanatory. Second, flow learning is not the same thing as populating an entry.

a. "Upon successful allocation" means "after successful allocation."

Claims 1 and 3 of the '125 patent and 1, 9 and 17 of the '311 patent require that the packet be forwarded for flow learning "***upon*** successful allocation of a new entry in the packet flow cache." Kent Decl., Ex. 2, '125 patent; Ex. 3, '311 patent (emphasis added). The claim thus requires that ***first*** a new entry is "allocated" in the packet flow cache (which has limited space), and only ***then*** is the packet forwarded for flow learning. PAN's proposed construction makes this requirement explicit; Fortinet simply repeats the words of the claim in its proposed construction, and ignores the issue in its Opening Claim Construction Brief ("Fortinet Cl. Constr. Br."). As a result, it is not clear whether Fortinet disputes the temporal limitation in the claim. It should not reasonably be subject to dispute that the packet is forwarded for flow learning only ***after*** "successful allocation" of a new entry in the packet flow cache. The phrase "upon completion of the assignment, the professor graded the papers" means that grading happened ***after*** the student completed the assignment: The professor did not grade the papers before completion of the assignment or while the student worked on the assignment. Indeed, the word "successful" is telling: you can't know whether an event has been successful until it is over, so the packet can't be forwarded "upon ***successful*** allocation" until ***after*** that allocation has taken place. The '311 specification is consistent with this plain meaning. Allocation takes place before forwarding: "When the PFE controller detects a new flow, it attempts to allocate one or more [entries in the packet flow cache]…. The PFE ***then*** forwards the packet to software using a descriptor marking of FWD_NEW." Kent Decl., Ex. 3, '311 patent at 8:14-22 (emphasis added).

b. To "allocate" a cache entry for a new flow means to create a new entry identifying that flow.

It is also unclear whether the parties disagree about the meaning of the phrase "successful allocation of a new entry of the packet flow cache for the new VR flow." Fortinet declines to provide a construction, arguing that the phrase "simply means what it says and would be easily understood by one of ordinary skill in the art." Fortinet Cl. Constr. Br., Docket No. 67 at 14. In its brief, while Fortinet does not say what it thinks the plain meaning of the term "allocation" is, Fortinet provides an example: "[f]or example, a spreadsheet table of rows and columns can be created prior to the time the entries on

the table are allocated to specific subject matter (*e.g.*, units sold, revenue, cost, etc.)." *Id.*

To the extent that this example reflects an implicit construction, PAN agrees with it. To "allocate" a new cache entry means to assign a particular slot in the cache to a particular flow. Using Fortinet's spreadsheet example, consider a spreadsheet of student papers and their associated grades. The spreadsheet contains blank, unallocated space. Here, the last row in the following spreadsheet has not yet been allocated:

Paper	Grade
Science of Firewalls	A
Router Basics	B

By contrast, the last row in the following spreadsheet has been allocated for a particular new paper, and thus a new entry has been created, although that entry has not yet been fully populated because the paper has not yet been graded:

Paper	Grade
Science of Firewalls	A
Router Basics	B
Anti-spam Techniques	

This understanding of "allocation" is supported by the specification, which describes the allocation process in detail. Allocation of flow cache entries (which the specification calls "Flow Cache Blocks" or "FCBs") is important, since there are only four FCBs available. The specification explains that, "[w]hen the PFE controller detects a new flow, it attempts to allocate one of four FCBs selected using its hashed flow index." Kent Decl., Ex. 3, '311 patent at 8:13-15. If an FCB is available, it is allocated to the particular flow by replacing the FCB's "tag fields" to identify the FCB as reserved for this particular flow: "If the PFE finds an available FCB, it replaces the FCB tag fields, sets the FwdAction field to pending, and increments the FCB pending tag." *Id.* at 8:15-17. If an FCB is not available, these allocation actions do not occur: "If the PFE is unable to allocate an FCB, it forwards the packet to software using a descriptor marking of FWD_COLLISION." *Id.* at 8:22-24.

c. Flow learning is the process of determining how to treat the packets, not populating a cache entry with the result of that process.

PAN's construction reflects that "flow learning" is the process of analyzing packets in a flow to learn how that flow should be treated. Fortinet contends, by contrast, that "flow learning" refers not to learning about flows, but instead to "populating the new entry" in the flow cache with the *result* of that learning process. This is contrary to common sense and common usage: learning about a subject is different from recording the results of that learning process. A census taker, for example, learns a person's name, then writes it down on a form. The "learning" takes place when the census taker asks for and receives the name; populating the form with the information learned is not, itself, "learning."

This common sense proposition is supported by the available evidence in the specification. "Flow learning" is not defined—and, indeed, is not discussed in any detail—in the specifications of the '125 and '311 patents. There are no substantive references to "flow learning" in the specification of the '311 patent at all. In the specification of the '125 patent, the only reference to "flow learning" is a reference to "previously stored flow learning results." Kent Decl., Ex. 2, '125 patent at 15:17. The '125 specification thus supports the distinction between the act of flow learning and the population of a cache entry with the results of that flow learning.

This distinction between flow learning and the population of the flow cache entry is also supported by the specification of United States Patent No. 7,340,535 ("'535 patent"), incorporated by reference into the specifications of the '125 and '311 patents, upon which Fortinet heavily relies. That specification draws a sharp distinction between flow learning and populating the flow cache entry (which the '535 patent calls "flow setup"): "According to the present example, there are three major elements to the process of pushing flows into hardware by the PFE driver: (a) New flow identification (b) *Learning* (c) *Flow setup*." Kent Decl., Ex. 6, '535 patent at 5:52-7. The '535 specification makes clear that "learning" refers to the collection of information about a flow, and that populating the allocated entry in the flow cache is a separate "flow setup" step:

> **Learning** is accomplished as the packet traverses the software IP forwarding stack using the PFED [Packet Forwarding Engine Driver] API functions. **The information collected is held in a buffer** referred to as an 'annotation buffer' which is allocated and attached to all learning packets before being passed to the software stack. **Flow setup is automatically**

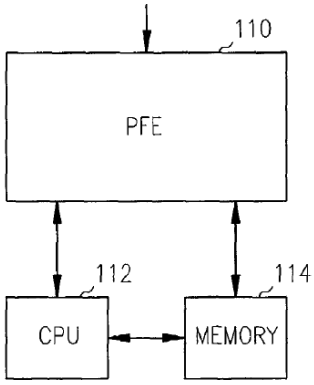
handled by the PFE driver when a learning packet is being forwarded.

Id. at 5:66-6:10 (emphasis added). This intrinsic evidence shows that "flow learning" does not mean "populating the new entry" in the flow cache, but instead means the process of learning about the flow.

d. The packet must be forwarded to a separate processor.

Claim 1 and 3 of the '125 patent and claims 1 and 9 of the '311 patent require "forwarding the packet to software on the processor for flow learning." "Forwarding" means sending the packet from one location to another. The claim requires that forwarding to take place "upon successful allocation of a new entry of the packet flow cache for the new VR flow." Thus, the plain and ordinary meaning of this phrase requires forwarding the packet from the circuitry that performs the required "successful allocation of a new entry of the packet flow cache for the new VR flow" to a separate location.

The specifications of the two patents describes the packet's path through the system in detail. The specification of the '311 patent explains that: "[o]n a cache miss, the ingress controller allocates a cache entry and forwards the packet to software on processor 112 for flow learning." Kent Decl., Ex. 2, '311 patent at 6:26-28. The "ingress controller" is part of the Packet Forwarding Engine, or "PFE." *Id.* 4:58-59. Figure 1 demonstrates that PFE 110 and processor 112 are indeed separate:



The PFE does the forwarding. The processor does the flow learning. Each is separate from the other.

///

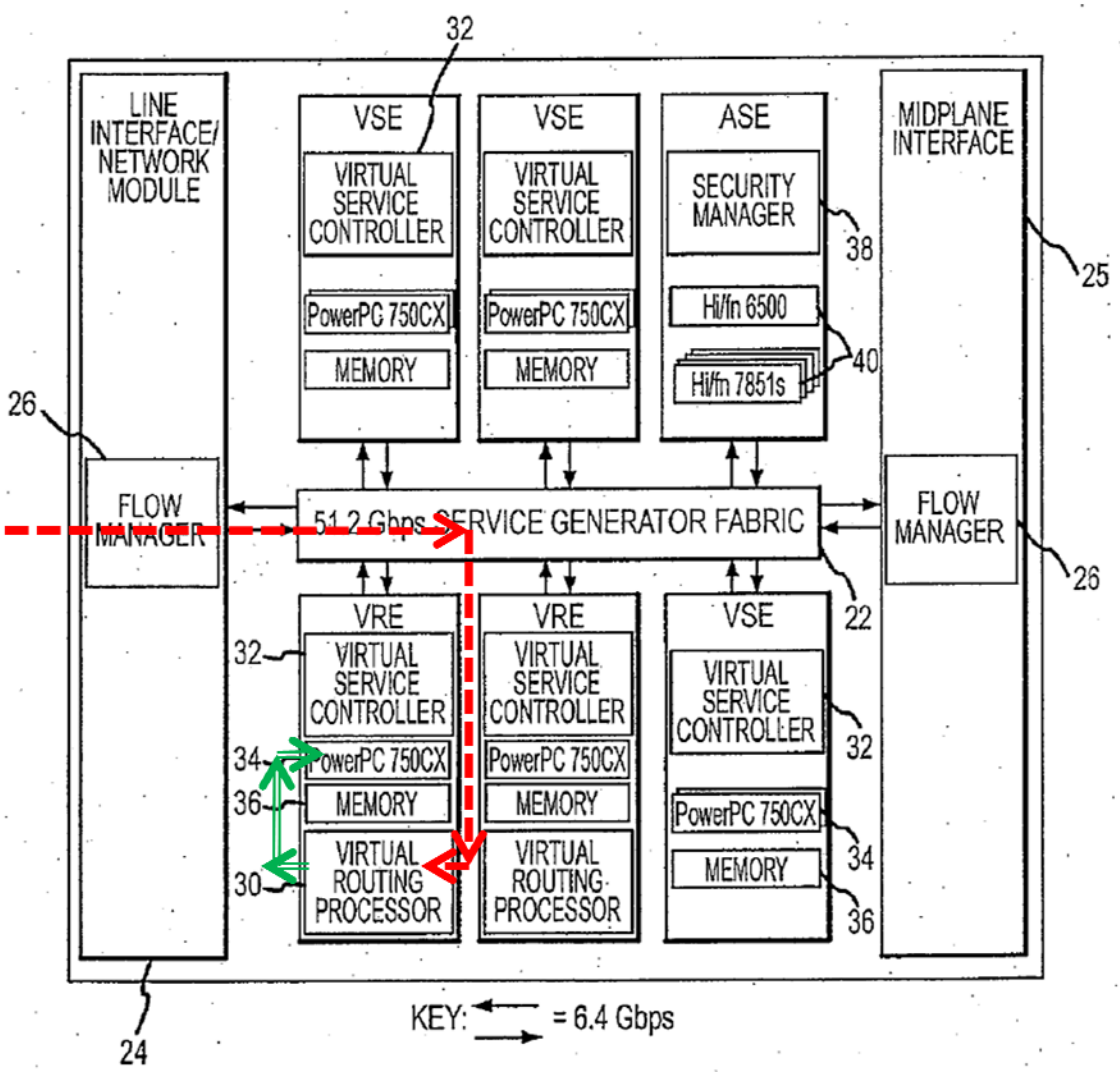
///

///

///

///

The '125 specification similarly explains that a packet "typically arrives from a Line Interface/Network Module 24 through the Service Generator Fabric 22 into one of the packet classifiers in the Virtual Routing Processor 30." Kent Decl., Ex. 2, '125 patent at 11:22-24. This path is shown in the red dotted line overlaid below on Figure 4 from the '125 patent:



Upon successful allocation of a new entry in the flow cache by the Virtual Routing Processor, the packet is forwarded to "[s]oftware running on the CPUs 34" for flow learning, as shown in the green double line overlaid on the above figure. Kent Decl., Ex. 2, '125 patent at 11:55. Here, too, the specification confirms that the packet is forwarded to a separate processor for flow learning.

Fortinet offers no definition of "the processor," apparently hoping to argue that "the processor" can refer to the same circuitry that also allocated a new entry in the flow cache. That cannot be so. The

claim requires after "successful allocation of a new entry," "forwarding . . . to the processor for flow learning." Having the same circuitry both allocate a new entry and perform flow learning would read the verb "forwarding" out of the claim.

e. A cache is an intermediate memory

The parties dispute what the word "cache" means in the phrase "packet flow cache." Fortinet contends that a "cache" can be any memory, so long as its contents are stored only "temporarily." Fortinet apparently hopes to argue that even a processor's main memory can be called a "cache," since all memory is, in some sense, "temporary." Fortinet's proposed construction is inconsistent with the plain and ordinary meaning of a cache. For example, the Comprehensive Dictionary of Electrical Engineering provides the following definition of "cache:"

> ***[A]n intermediate memory store*** having storage capacity and access times somewhere in between the general register set and main memory. The cache is usually invisible to the programmer and its effectiveness comes from being able to exploit program locality to anticipate memory access patterns and to hold closer to the CPU: ***most access to main memory can be satisfied by the cache***, thus ***making main memory appear to be faster than it actually is***.

Kent Decl., Ex. 10, CDEE at PAN017147 (emphasis added). This intermediate memory structure serves to satisfy the need for most—but not all—access to the main memory. By anticipating memory access patterns and by virtue of its intermediate location, the cache is designed to permit faster access to data than would be possible from the main memory.

The patent specifications confirm that the claims used the term "cache" in its customary sense. *See*, *e.g.*, Kent Decl., Ex. 3, '311 patent at 5:4-6 ("both the PFE ingress and egress units comprises [sic] an array of 32-bit packet processors 206 that share an on-chip write-back cache 212."); Ex. 2, '125 patent at 11:29-33 ("The packet classifier [in the Virtual Routing Processor 30] executes micro-code instructions to extract bit and byte fields and even perform Boolean functions for this purpose. In one embodiment, a hash function is applied to the contents of the fields to obtain an address into a flow cache storing a predetermined number of forward indexes."). The main memory is depicted separately from these caches. *See* Kent Decl., Ex. 2, '125 patent, Fig. 4 (depicting memory 36 as separate from Virtual Routing Processor 30); Kent Decl., Ex. 3, '311 patent , Fig. 1 (depicting memory 114 as separate from

Packet Forwarding Engine 110). Thus, the cache is an intermediate memory location separate from the main memory.

2. "store/storing the network traffic content in a stack when the protocol of the network traffic content matches the prescribed protocol"

TERM OR PHRASE	FORTINET'S PROPOSED CONSTRUCTION AND SUPPORT	PAN'S PROPOSED CONSTRUCTION AND SUPPORT
store/storing the network traffic content in a stack when the protocol of the network traffic content matches the prescribed protocol ('990 patent)	store/storing the network traffic content in memory for temporary storage when the protocol of the network traffic content matches recognized protocol	store/storing the network traffic content in memory for temporary storage when the protocol of the network traffic content matches one of the set of protocols that have been pre-identified as potentially containing content desired to be detected

The parties agree about the proper construction of this phrase except for the definition of "the prescribed protocol." This remaining dispute is addressed in the following section.

3. "a prescribed protocol of network traffic content that could contain content desired to be detected"

TERM OR PHRASE	FORTINET'S PROPOSED CONSTRUCTION AND SUPPORT	PAN'S PROPOSED CONSTRUCTION AND SUPPORT
a prescribed protocol of network traffic content that could contain content desired to be detected ('990 patent)	a recognized protocol of network traffic content that could contain content desired to be detected	any protocol that has been pre-identified as potentially containing content desired to be detected

The dispute here is what it means to be "prescribed." The word "prescribed" comes from Latin; "pre" means before, and "scribere" means to write. Kent Decl., Ex. 11, The American Heritage Dictionary of the English Language, Fourth Edition. Houghton Mifflin Company, 2004. http://dictionary.reference.com/browse/prescribe (accessed: June 18, 2010). To pre-scribe thus derives from "to write before." In modern usage, to "prescribe" means "to set down as a rule." *Id.* The claim refers to a "prescribed" protocol; a protocol that has been prescribed is a protocol that has been set down by rule.

Fortinet asserts that a "prescribed" protocol is any "recognized" protocol. Prescribed and recognized do not mean the same thing, and Fortinet does not provide any support for its assertion that they are synonymous. Fortinet is proposing this construction because it hopes somehow to argue that PAN's products can infringe even though the PAN system handles all protocols in the same way with respect to content desired to be detected. Fortinet's construction erases the important distinction between protocols that have been pre-identified as potentially containing content desired to be detected and other protocols which, while they may be recognized, have not been pre-identified as potentially containing content desired to be detected.

Claim 1 requires "determin[ing] whether a protocol of the network traffic content matches a prescribed protocol of network traffic content." Kent Decl., Ex. 4, '990 patent at 23:27-29. In order to make such a determination, there must be a pre-identified protocol to which incoming network traffic can be compared. That protocol has been pre-identified *because* it could contain content desired to be detected. The system processes the network traffic based on whether it matches that prescribed protocol. It stores "the network traffic content in a stack when the protocol of the network traffic content matches the prescribed protocol." *Id.* at 23:32-34. It performs "filtering of the network traffic if the type of the network traffic content does not match the prescribed type." *Id.* at 23:35-37. In other words, traffic is treated differently depending on whether or not it matches the prescribed protocol or type "of network traffic content that could contain content desired to be detected."[5]

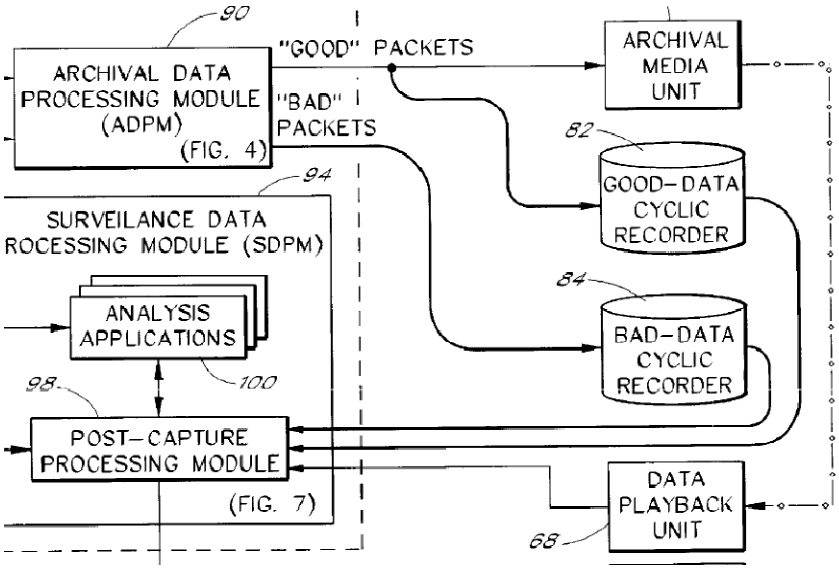
The specification confirms this proposition. The specification identifies a protocol differentiator that has rules that pass network traffic of different protocols either for packet processing or to a stack as:

> Next, depending on the type of content received or the content protocol, protocol differentiator 704 passes the network traffic data to ***either*** packet processing module 706 ***or*** stack 708. For example, certain types of network traffic content, such as DNS data or telnet data, may be considered "safe" traffic content, while other types of network traffic content, such as HTTP content or emails, may be considered as "unsafe" traffic content (i.e., content that may contain virus, worms, or undesirable material). In the illustrated embodiments, protocol differentiator 704 is configured to pass safe traffic content to packet processing module 706, and unsafe traffic content to stack 708.

[5] The relationship between "protocol" and "type" in the claims is confusing, and not at issue here. The best reading of the claims is that "type" is broader than "protocol," and includes such characteristics as the port associated with the traffic. Kent Decl., Ex. 4, '990 patent at 26:15-29.

Id. at 8:26-51 (emphasis added). The protocol differentiator has rules identifying in advance which protocols are considered "safe" or "unsafe." Indeed, the specification explains that, in some embodiments, a user can configure or program these rules, which are actions that occur in advance of determining a protocol match. *Id*. at 8:59-62 ("[P]rocessor 702 may be programmable or configurable such that a ***user can prescribe*** certain types of network traffic content to be passed to packet processing module 706 or to stack 708.") (emphasis added).

Finally, the file history of the '990 patent explicitly disclaims any invention where all protocols are treated the same way. During prosecution, the Examiner issued a prior art rejection over a prior art patent, U.S. Patent No. 6,453,345, whose lead inventor was Trcka ("Trcka Patent"). Kent Decl., Ex. 13, October 3, 2007 Office Action at 2. The Trcka patent described determining whether incoming network traffic is "good" or "bad" traffic and storing the "bad" traffic in a "Bad-Data Cyclic Recorder." The figure below depicts the Trcka disclosure:



Kent Decl, Ex. 13, Trcka Patent at 12:12-16, 34-37, 41-50; 14:7-16. In Trcka, the Surveillance Data Processing Module—the second processor—used "prespecified criteria to analyze data read in from the Good-Data Cyclic Recorder 82 and/or the Bad-Data Cyclic Recorder 84" to "automatically detect security breaches, inbound viruses, and other anomalies during or shortly after . . . ." *Id.* at 13:1-8. Based on Trcka, the Examiner concluded that the only element missing from then-pending claim 1 was

that Trcka did "not explicitly teach that the modules be implemented as hardware or processor based modules," which the Examiner found "would have been obvious to one of ordinary skill in the art at the time of invention" in light of another reference. Kent Decl., Ex. 12, October 3, 2007 Office Action at 4.

In response, Fortinet amended its claims to specify that the first processor must "perform filtering of the network traffic if the type of the network traffic content does not match the prescribed type." Kent Decl., Ex. 14, December 14, 2007 Amendment and Response to Office Action at 2. Citing that new claim element, Fortinet argued that Trcka does not "disclose or suggest that the first processor performs filtering of the network traffic if the type of the network traffic content *does not match* the prescribed type, and the second processor configured to determine whether the network traffic content contains the content desired to be detected if the type of the network traffic content *matches* the prescribed type." *Id.* at 9 (emphasis in original). In particular, Fortinet argued that Trcka did not meet these limitations because the first processor passed both the prescribed type of network traffic ("bad" packets) and the non-prescribed type of network traffic ("good" packets) to the claimed second processor:

> Rather, Trcka discloses that **both "GOOD" and "BAD" packets are analyzed by the *same* Surveillance Data Processing Module** (SDPM) 94, which the Office Action analogized as the claimed "second processor" (figure 3). Thus, to the extent that the "GOOD" and "BAD" packets are considered different types, these "GOOD" and "BAD" packets are **not routed to different processors based on whether the type matches a prescribed type**.

Id. at 9 (bold emphasis added). Fortinet reiterated in other statements to the Examiner that its invention required that prescribed and non-prescribed traffic be treated differently. *See also* Kent Decl., Ex. 15, July 15, 2008 Amendment and Response at 8 (The invention is drawn to a device having "a first processor that performs certain functionality and a second processor that performs other functionality.").

Fortinet cannot reclaim the claim scope that it disavowed. "The doctrine of prosecution disclaimer is well established in Supreme Court precedent, precluding patentees from recapturing through claim interpretation specific meanings disclaimed during prosecution." *Omega Eng'g, Inc. v. Raytek Corp.*, 334 F.3d 1314, 1323 (Fed. Cir. 2003). For example, in *Southwall Technologies, Inc. v. Cardinal IG Co.*, the Federal Circuit held that the limitation "sputter-deposited dielectric" excluded a two-step process, because the patentee argued during prosecution that the metal oxide in the process was

"directly deposited." 54 F.3d 1570, 1574-77 (Fed. Cir. 1995). The Federal Circuit found that argument to "necessarily disclaim[] the examiner's interpretation of 'sputter-deposited' metal oxides as encompassing a two-step process in which metal is first deposited as a metal and then oxidized." *Id.*; *see also AccuScan, Inc. v. Xerox Corp.*, 76 Fed. Appx. 290, 292 (Fed. Cir. 2003) (Because "during prosecution, the patentee had distinguished the invention over the prior art, including the Krallinger reference, by emphasizing the importance of storing a sample of the white signal," the claims required continuous storing—even though the plain language would not have compelled that result).

The same is true here. To obtain issuance, Fortinet explicitly disclaimed systems where all protocols were sent on for further analysis. Fortinet thus necessarily disclaimed any interpretation of a "prescribed" protocol that does not distinguish between protocols based on whether they have been identified as having content desired to be detected.

4. "eliminating the other state of classification as a potential classification candidate for the second packet"

TERM OR PHRASE	FORTINET'S PROPOSED CONSTRUCTION AND SUPPORT	PAN'S PROPOSED CONSTRUCTION AND SUPPORT
eliminating the other state of classification as a potential classification candidate for the second packet ('974 patent)	eliminating the other state of classification from consideration for a packet that is subsequent to the first packet analyzed	eliminating the other state of classification from consideration and thereby not considering all potential classifications that otherwise could be considered for the second packet

PAN agrees that the terms "first" and "second" are used in their ordinal sense. The "second" packet could be any packet that is separate from and subsequent to the "first" packet. For this reason, PAN has no objection to incorporating this concept into its construction as follows:

> The second packet is a packet that is subsequent to the first packet analyzed.

This construction would make clear that each reference to "the second packet" in the claims refers consistently to the same packet.

The only remaining point of dispute is how to construe the requirement of eliminating a state of

classification "as a potential classification candidate." Fortinet's position is that this requires nothing more than eliminating a state of classification from consideration. But Fortinet's construction strips an important idea out of the claim. The state of classification that was eliminated must have been a potential classification candidate when it was eliminated. In other words, there must be a potential classification that could have been considered, but wasn't, because it had been eliminated. That is why PAN's construction requires "eliminating the other state of classification from consideration *and thereby not considering all potential classifications that otherwise could be considered.*"

This construction is required not just by the claim, but also by the prosecution history. Indeed, PAN's proposed construction is taken almost verbatim from the applicants' own words. In response to an examiner rejection, the applicants amended their claims to add the words "potential classification" and argued that the prior art failed to disclose the claimed "negative classification" because it did not include "classifying the second packet of the session by eliminating the other classification from consideration. As a result, the classifying can be performed more quickly because not all potential classifications need to be considered." Kent Decl., Ex. 7, 12/18/2008 Amendment at 7. The examiner then allowed the claims and commented that "[t]his communication warrants no examiner's reason for allowance, as applicant's reply makes evident the reasons for allowance, satisfying the record as whole [sic] as required by rule 37 CFR 1.104(e)." Kent Decl., Ex. 8, Notice of Allowability at 6. *See, ACCO Brands, Inc. v. Micro Sec. Devices, Inc*., 346 F.3d 1075, 1079 (Fed. Cir. 2003) ("the examiner's Reasons for Allowance make clear that the examiner and the applicant understood" the claims to have a certain meaning).

5. "unknown destination"

TERM OR PHRASE	FORTINET'S PROPOSED CONSTRUCTION AND SUPPORT	PAN'S PROPOSED CONSTRUCTION AND SUPPORT
unknown destination ('272 patent)	unspecified destination	a destination that has not yet been determined

Claims 1 and 68 of the '272 patent require receiving a communication that has "content for an unknown destination," while claim 43 phrases the same requirement as "the content of a received communication for an unknown destination." Claim 78 requires "ascertaining a meaning of at least a

portion of the communication for an unknown destination." The only dispute is whether "unknown" means "unspecified" or "not yet determined."

Claim construction always begins with the words of the claims. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed.Cir. 2005) (en banc). The word "unknown" does not have any special meaning in the '272 patent, nor is it a technical term such that the Court needs to consult other sources of information to determine what it means. "Unknown" means "not known." "Unknown" does not mean "unspecified." Indeed, the patentee knew the difference between "specified" and "known." In claims 2, 44, and 75, the patentee chose to use the word "specified" in the phrase "a ***specified*** device of the destination." Kent Decl., Ex. 5, '272 patent at 13:7, 15:25, 17:38 (emphasis added). The patentee made a deliberate choice to use the word "specified" instead of the word "known" in those claims, just as the patentee made a deliberate choice to use the word "unknown" instead of the word "unspecified" in the claims at issue here.

Nothing in the specification varies the plain meaning of the word "unknown." To the contrary, the specification repeatedly reinforces that the purpose of the invention is to determine the destination for incoming communications.[6] *See* Kent Decl., Ex. 5, '272 patent at 1:49-51 ("in order to determine the proper destination"); *id*. at 2:48-50 ("selecting a destination based on the values assigned in the assigning step…"); *id*. at 2:63-4 ("instructions for selecting a destination based on values assigned in the assigning step"); *id*. at 2:66-3:3 ("selecting a destination based on the results of the applying step"); *id*. at 8:30-33 (destination "determined based on predefined rules as applied to the value matrix assigned").

The specification also makes clear that the "unknown destination" includes more than "unspecified" destinations. For example, when someone places a telephone call, a destination is specified by the phone number dialed by a caller. However, the ultimate destination of the call may be unknown, because the caller may call a general number, but want to be routed to a specific individual. The system considers the call to be for an "unknown destination," and then attempts to determine the

[6] Indeed, Fortinet's own proposed construction for the claim term "translational language" – "a matrix that can be used to **determine the destination** for a communication" – implicitly concedes that the invention attempts to determine the destination for communications where those destinations have not yet been determined.

particular destination for the call or the call's content. Kent Decl., Ex. 5, '272 patent at 5:4-8 ("If the caller requests a particular person, the person can be selected from the list of persons in field 232 of call reception screen 200 in step 106, the call will be routed, i.e. directed, to the selected person in step 108 when the receptionist selects transfer button 240, and the process ends in step 110.").

In claims 1, 43 and 68, the ***content*** of the communication is "for an unknown destination." Consequently, the communication itself could specify one general destination and still have "content for an unknown destination" as required by the claims. For example, a communication directed to an accounting department (a "specified" destination) could contain content that the system determines needs to be routed to John Smith (a destination previously "unknown"). In that situation, the content was for an unknown destination (John Smith) even if the communication generally was to a specified destination (the department). *See* Kent Decl., Ex. 5, '272 patent at 8:35-36 ("destination can be a department, a person, a particular location or the like"). To use another example, the fact that the content of a suspected spam email is sent to a particular ("specified") email address does not mean that its ultimate destination, as between the user's mailbox and the user's spam folder, is "known" prior to analysis of that email by antispam algorithms.

6. "display/displaying/present/presenting/presentable"

TERM OR PHRASE	FORTINET'S PROPOSED CONSTRUCTION AND SUPPORT	PAN'S PROPOSED CONSTRUCTION AND SUPPORT
display/displaying/ present/presenting/ presentable ('272 patent)	make visible/making visible/ visible to a human user	plain meaning

There does not appear to be a dispute as to this limitation. It is not PAN's intent to argue that the claims are infringed where information is not displayed "to a human user." PAN simply believes that the claim terms are clear on their face, as they do not have any technical component, and therefore do not require construction.

///

///

7. "communication"

TERM OR PHRASE	FORTINET'S PROPOSED CONSTRUCTION AND SUPPORT	PAN'S PROPOSED CONSTRUCTION AND SUPPORT
communication ('272 patent)	Call	plain meaning

The '272 patent does not limit a "communication" to a "call." There are many other types of communications, and the '272 patent sought to claim them. As the specification explains:

> The classification method can be used for managing ***any type of communication***. For example, the invention can be used to classify and/or route facsimile messages or other printed documents, ***electronic mail messages***, instant electronic messages, or any other human readable or computer readable communication.

Kent Decl., Ex. 5, '272 patent at 12:32-8 (emphasis added). Where, as here, the patentee includes express language in the specification supporting a broad construction of a term such as "communication," the term should not be narrowly construed to exclude that which the patentee expressly intended to bring within the language of the claims. *Martek Biosciences Corp v. Nurtinova, Inc.*, 579 F.3d 1363, 1381 (Fed. Cir. 2009) (where the specification expressly stated that the invention extends to "any organism belonging to the kingdom Animalia," extensive discussion of farm animals did not exclude human animals from the scope of the claims).

Indeed, Claim 8, which depends from asserted Claim 1, requires transferring the "communication" to one of a series of devices, including "an e-mail system." One cannot transfer a call to an e-mail system, so Fortinet's construction cannot be correct.

To be sure, the handling of telephone calls is a preferred embodiment described in the specification. But the Federal Circuit has warned that courts cannot limit a patent's unambiguously broader claims to the preferred embodiment, absent a clear indication of intent on the part of the patentee. "[I]t is improper to read limitations from a preferred embodiment described in the specification – even if it is the only embodiment – into the claims absent a clear indication in the intrinsic record that the patentee intended the claims to be so limited." *Enzo Biochem, Inc v. Applera Corp.*, 599 F.3d 1325, 1342 (Fed. Cir. 2010) (quoting *Liebel-Flarsheim Co. v. Medrad, Inc.*, 358 F.3d 898, 913 (Fed. Cir. 2004)).

Fortinet has not pointed to any such clear indication here.

In the face of the specifications' express statement that the claims are not limited to calls, but also encompass emails, Fortinet argues that this disclosure is not enabling and that *for this reason* the court should limit the scope of the claims. Plaintiff Fortinet, Inc.'s Motion for Summary Judgment of Noninfringement at 13-14, Docket No. 46 ("[N]o definition of 'communication'… other than 'call' could possibly be enabled."). Not only is the enablement point wrong,[7] but enablement is not the inquiry before the Court.

Courts cannot rewrite the words chosen by the patentee. *Helmsderfer v. Bobrick Washroom Equip., Inc*., 527 F.3d 1379, 1383 (Fed. Cir. 2008) ("Courts do not rewrite claims; instead we give effect to the terms chosen by the patentee.") (quoting *K-2 Corp. v. Saloman*, 191 F.3d 1356, 1364 (Fed. Cir. 1999). This is true even when one party argues that the claim is invalid, unless the claim term in question is ambiguous. *Broadcom Corp. v. Qualcomm Inc.*, 543 F.3d 683, 690 (Fed. Cir. 2008) ("While we have acknowledged the maxim that claims should be construed to preserve their validity, we have not applied that principle broadly…. Instead, we have limited the maxim to cases in which the court concludes, after applying all the available tools of claim construction, that the claim is still ambiguous.") (quoting *Phillips*, 415 F.3d at 1327). The phrase "communication" is not ambiguous, and the enablement argument is an attack on the patent's validity rather than argument about what the claims should mean.

Fortinet also argues that communication should be limited to call because the examiner appeared, at times, to use the term "call" and the term "communication" interchangeably. But the patentee never distinguished prior art on the ground that a communication was limited to a call, and the examiner never

[7] Fortinet does not perform an enablement analysis. It does not offer any testimony from a person of skill in the art as to whether such a person could practice the invention as claimed. Instead, it counts the number of times the word "call" occurs in the specification, compares that to the number of times "electronic mail" occurs, and then concludes that because one is discussed extensively and the other is not, that therefore necessitates a conclusion that the other is not enabled. Needless to say, that is not the enablement test. Where, as here, a genus (communications) is claimed, and a species (calls) is described in greater detail, an enablement analysis must evaluate whether a person of skill in the art could have practiced other species (electronic mail), rather than presume that they are not enabled. *See, e.g.*, *Amgen Inc. v. Hoechst Marion Roussel, Inc.*, 314 F.3d 1313, 1336-37 (Fed. Cir. 2003) (while "disclosure of one or two species *may* not enable a broad genus," the genus is enabled where the factual record shows that "any gaps between the disclosures and the claim breadth could be easily bridged" by one of skill in the art at the time of the invention).

indicated that the invention was limited to a call. Instead, the examiner used a "call" as one example of a "communication" in mapping a prior art reference to the claims. For example, Fortinet argues that the Court should draw an inference from the fact that the examiner explained that "Anderson teaches a method for managing communications comprising the steps of: receiving an incoming call (communication)." Anderson is a prior art system that received an incoming call. The examiner simply indicated, in the passage quoted by Fortinet, that the "incoming call" in Anderson mapped to the "communication" required by the claims. Kent Decl., Ex. 16, 6/16/2003 Amendment at PAN000178-79 (describing Anderson as relating to a call). Nor did the applicants' response concede that a communication is limited to calls; it characterized the prior art relating to calls as not disclosing its invention related to communications:

> ***The invention leverages*** what applicant believes to be one of humankind's greatest abilities – ***the ability to understand and process human communication***. Systems using the invention feature that human ability, and make other actions required in handling data and communication purely systematic. Anderson and other prior art systems take the opposite approach, teaching away from the claimed invention entirely. ***In particular, the prior art seeks***, by utilization of computerized processes to the greatest extent possible, ***to automatically understand what the call is and how it is to be directed***.

Id. at PAN000179 (emphasis added). There can be no prosecution disclaimer on this record. *Omega*, 334 F.3d at 1323-24 (prosecution disclaimer requires "specific meanings" to have been "unequivocally disavowed").

8. "translational language"

TERM OR PHRASE	FORTINET'S PROPOSED CONSTRUCTION AND SUPPORT	PAN'S PROPOSED CONSTRUCTION AND SUPPORT
translational language ('272 patent)	matrix that can be used to determine the destination for a communication	tool for grouping communications based on equivalent but non-identical content

Of the asserted claims, only claims 68 and 78 recite the phrase "translational language," and the phrase does not form the basis of any argument in Fortinet's Motion for Summary Judgment of Noninfringement with respect to the '272 patent. In each of those claims, a "translational language" is

applied "to the communication to determine a destination for the communication." Neither party disputes that the translational language determines the destination for a communication.

This is consistent with the prosecution history, where the patentee explained that a translational language provided two components—characteristics of communications and possible values for each characteristic—to be used in determining the destination of the communication:

> The invention relates to a system for determining the appropriate destination of communications, such as telephone calls, based on the content of the communication. A translational language is applied to the communication to facilitate determination of the destination. **The translational language provides a relatively small predetermined set of communication characteristics that are relevant to the destination determination and general treatment of the communication and a relatively small predetermined set of possible values for each characteristic**. This permits a human operator to readily translate the content of a communication into a reduced and succinct language.

Kent Decl., Ex. 16, 6/16/2003 Amendment at PAN000172 (emphasis added).

There does not appear to be a substantive dispute between the parties regarding the meaning of this claim term. PAN does not disagree, in theory, that a translational language is a "matrix that can be used to determine the destination for a communication"—but PAN is concerned that the use of the term "matrix" could confuse the jury.

The translational language is a "matrix" in the sense that there is a relationship between inputs (the content of a communication) and outputs (a destination to which that communication is to be sent), via an intermediate translational step (the communication's characteristics). This understanding of the term "matrix" comports with the specification's broad use of the term "matrix" to include a list (that is, a one-dimensional matrix): "As noted above, the content of a call is determined by assigning values to a plurality of characteristics thereby creating a value matrix, i.e. a list of selected values."). Kent Decl., Ex. 5, '272 patent at 8:42-44.

As a result, PAN is willing to agree that a translation language is a "matrix (e.g., a list) that can be used to determine the destination for a communication."

///

///

IV. CONCLUSION

For these reasons, PAN's proposed constructions should be adopted, and Fortinet's should not.

Dated: June 18, 2010

Respectfully submitted,

By: /s/ Ryan M. Kent
RYAN M. KENT

Attorneys for Defendants - Counterclaim Plaintiff PALO ALTO NETWORKS, INC. and Defendant PATRICK R. BROGAN

CERTIFICATE OF SERVICE

I certify that all counsel of record is being served on June 18, 2010 with a copy of this document via the Court's CM/ECF system.

Michael A. Ladra	mladra@wsgr.com
James C. Yoon	jyoon@wsgr.com
Stefani E. Shanberg	sshanberg@wsgr.com
Robin L. Brewer	rbrewer@wsgr.com

Dated: June 18, 2010

DURIE TANGRI LLP

By: /s/ Ryan M. Kent
Ryan M. Kent

Attorneys for Defendants – Counterclaim Plaintiff PALO ALTO NETWORKS, INC. and Defendant PATRICK R. BROGAN